
# Procesamiento de Eventos Complejos para la detección de amenazas de seguridad

# >whoami

## Francisco López

- Ingeniero de Software @Virustotal
- Black Hat USA Arsenal,
  Hackers Week, OpenSouthCode,
  DevFest GDG Málaga

ECIJA

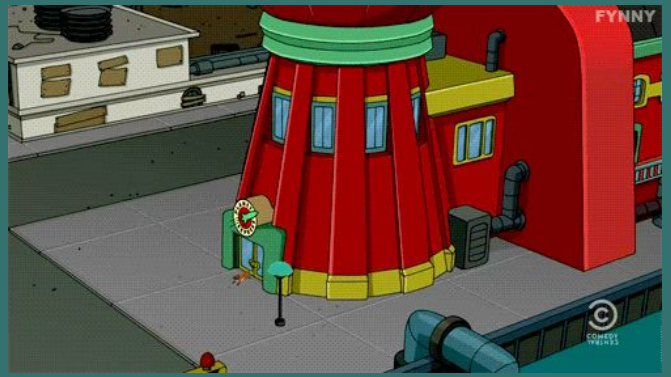
HISPASEC

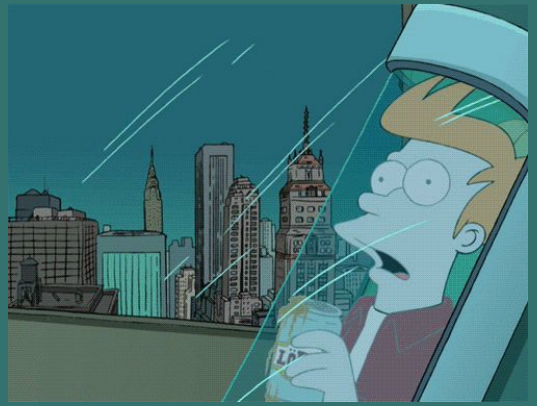
freepikcompany

# CEP

**C**omplex **E**vent **P**rocessing


POLICE


FYNNY



Saber qué ocurre

**CUANTO ANTES.**

Reaccionar de la forma más adecuada

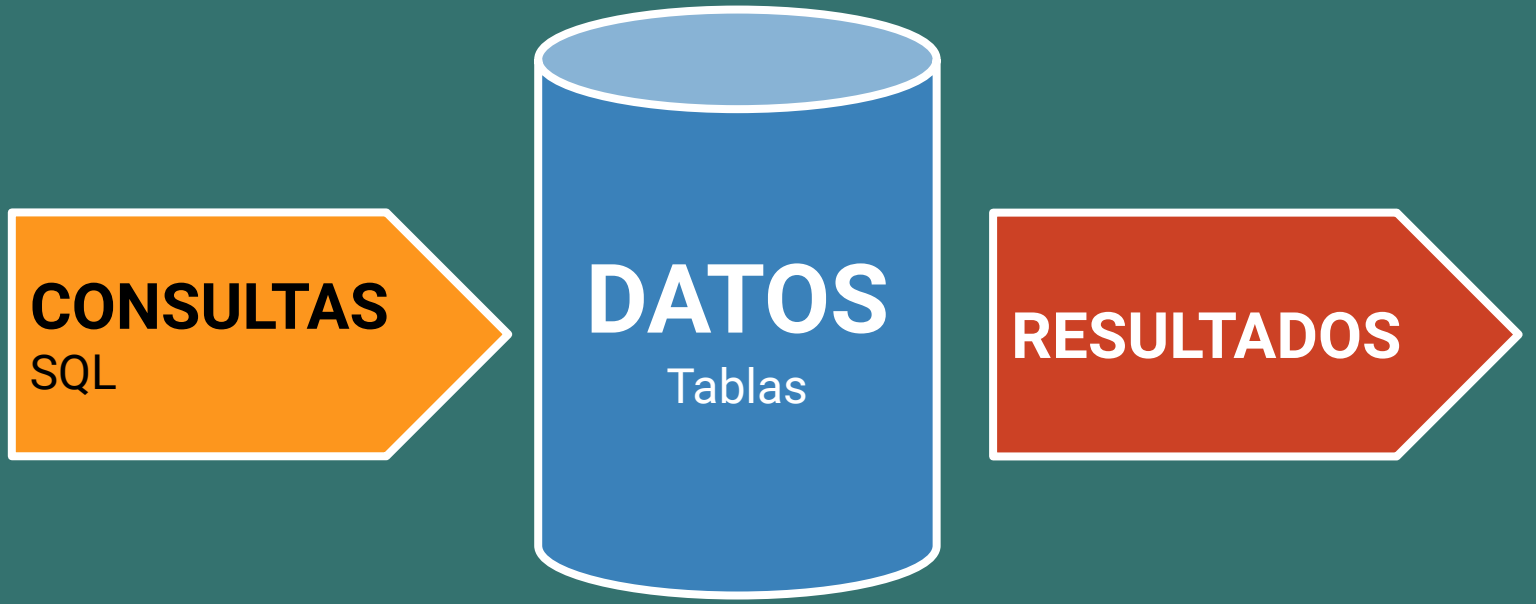
**CUANTO ANTES.**

*"Event processing is a method of tracking and analyzing streams of information about* ***things that happen****, and deriving* ***a conclusion*** *from them."*

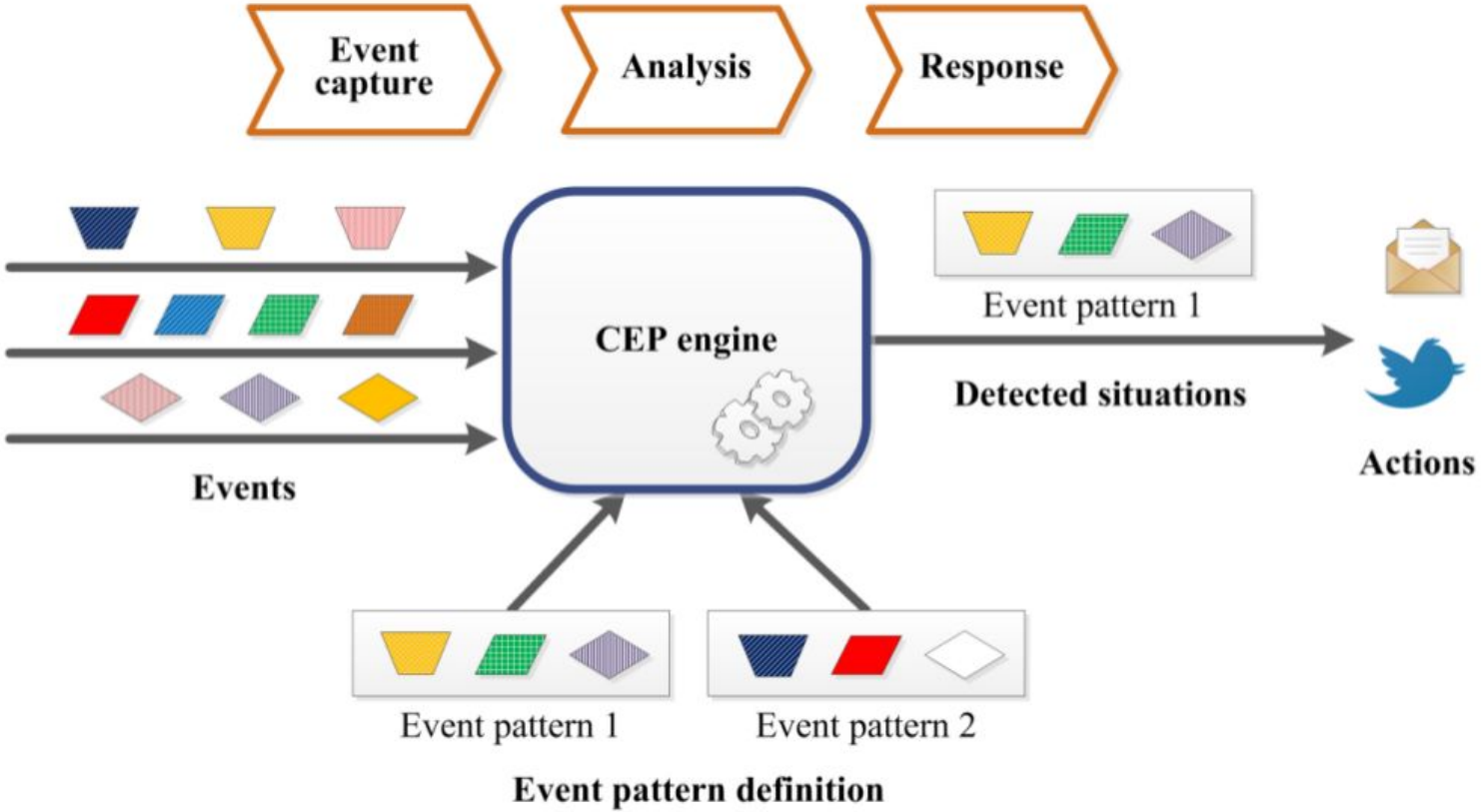
*"Complex Event Processing is event processing that combines* ***data from multiple sources*** *to infer events or patterns that* ***suggest more complicated circumstances.***"

*"The fact that a software system*
***must process and react to continual inputs from many sources (e.g., sensors)***
*rather than from human operators requires one to*
***rethink the fundamental architecture of a DBMS for this application area.***"

*Aurora: a new model and architecture for data stream management, 2003*


CONSULTAS
SQL
DATOS
Tablas
RESULTADOS


DATOS
Eventos
CONSULTAS
Patrones
RESULTADOS




*MEdit4CEP: A model-driven solution for real-time decision making in SOA 2.0.*
**Boubeta-Puig, Juan, Ortiz, Guadalupe y Medina-Bulo, Inmaculada.**

t = 5min

t = 5min

$t_1$

$t_2$

$t_3$

$t_4$

$t_5$

t = 5min

t1

t2

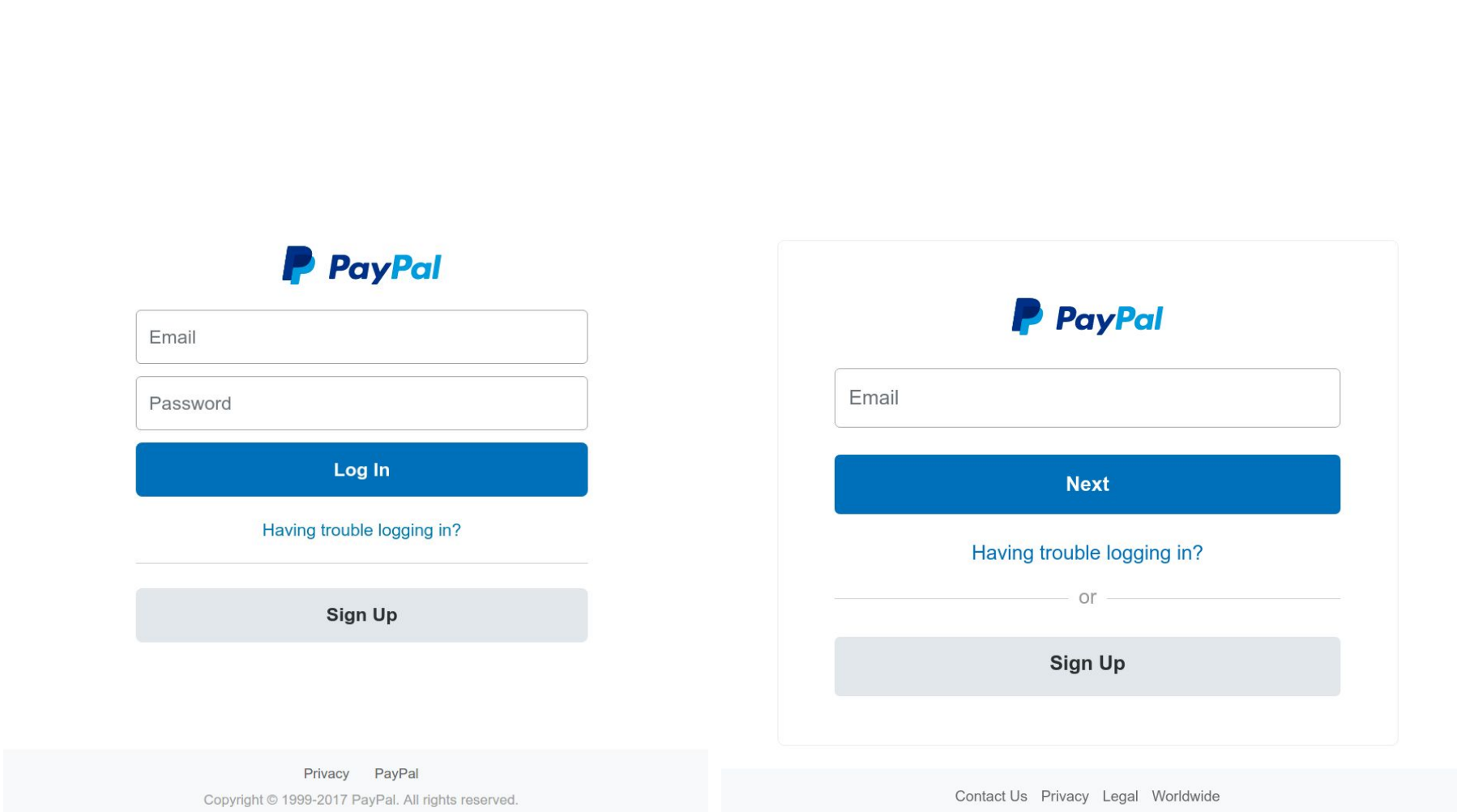
t3

t4

t5

t6

# DETECCION DE PHISHING


PayPal
Email
Password
Log In
Having trouble logging in?
Sign Up
Privacy PayPal
Copyright © 1999-2017 PayPal. All rights reserved.
PayPal
Email
Next
Having trouble logging in?
or
Sign Up
Contact Us Privacy Legal Worldwide

```
<!DOCTYPE html><!--[if lt IE 9]><html lang="en" class="no-js lower-than-ie9 ie"><![endif]--><!--[if lt IE 10]><html lang="en" class="no-js lower-than-ie10 ie"><![endif]--><!--[if !IE]>--><html lang="en" class="no-js"><!--<![endif]--><head><!--Script info: script: node, template:  , date: Jan 26, 2017 06:06:54 -08:00, country: AU, language: en web version:  content version:  hostname : wYtPaR9GtOjbsaEAFEsGi6rMsD0CQXWRlYbSobH92jCec1myAKRznqj5kLkwTpVKRRRfG00SmKY rlogid : BX%2FZx9Yh0MFxdY74Hm0lB%2B4F73WPzaSJ2KYKo%2B%2Bu93rhmyx3T23vq3WAx6hDR%2FVdKURmWgOuYrcJ06MSJd6ydhSrodyjO1G%2B_159db19be47 --><meta charset="utf-8" /><title></title><meta http-equiv="content-type" content="text/html; charset=UTF-8" /><meta name="application-name" content="PayPal" /><meta name="msapplication-task" content="name=My Account;action-uri=https://www.paypal.com/us/cgi-bin/webscr?cmd=_account;icon-uri=http://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico" /><meta name="msapplication-task" content="name=Send Money;action-uri=https://www.paypal.com/us/cgi-bin/webscr?cmd=_send-money-transfer&amp;send_method=domestic;icon-uri=http://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico" /><meta name="msapplication-task" content="name=Request Money;action-uri=https://personal.paypal.com/cgi-bin/?cmd=_render-content&amp;content_ID=marketing_us/request_money;icon-uri=http://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico" /><meta name="keywords" content="transfer money, email money transfer, international money transfer " /><meta name="description" content="Transfer money online in seconds with PayPal money transfer. All you need is an email address." /><link rel="shortcut icon" href="https://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico" />
<link rel="apple-touch-icon" href="https://www.paypalobjects.com/webstatic/icon/pp64.png" /><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1, user-scalable=yes" /><link rel="stylesheet" href="https://www.paypalobjects.com/web/res/06c/0effc0b788391963059a631dd9d03/css/app.css" /><!--[if lte IE 9]><link rel="stylesheet" href="https://www.paypalobjects.com/web/res/06c/0effc0b788391963059a631dd9d03/css/ie9.css" /><![endif]--><script src="https://www.paypalobjects.com/web/res/06c/0effc0b788391963059a631dd9d03/js/lib/modernizr-2.6.1.js"></script><style id="antiClickjack">body {display: none !important;}</style><script>/* Don't bust the frame if this is top window* or if the parent window is *.paypal.com domain (Checkout for example).*/if (self === top ||
```

```
<!DOCTYPE html><!--[if lt IE 9]><html lang="en" class="no-js lower-than-ie9 ie desktop"><![endif]--><!--[if lt IE 10]><html lang="en" class="no-js lower-than-ie10 ie desktop"><![endif]--><!--[if !IE]>--><html lang="en" class="no-js desktop"><!--<![endif]--><head><!--Script info: script: node, template:  , date: Oct 17, 2017 14:22:05 -07:00, country: US, language: en web version:  content version:  hostname : qy3yggRePoWYxeIZYO7Hqul8cwxyRO1BDRQ+yT8jV+zCUhdzT1PnOgk9drZe4lAzgcfid2ELc2k rlogid : fMf5ZgJF71UcY4ZHm2koNcgw8unO27ZYyb38fUyifpdCXZRZMXs2njKauHni95xczO8PKsyhZIoy3ngmc9yb1KEEbA8UEXd8_15f2c370b77 --><meta charset="utf-8" />
<title>Log in to your PayPal account</title><meta http-equiv="content-type" content="text/html; charset=UTF-8" /><meta name="application-name" content="PayPal" /><meta name="msapplication-task" content="name=My Account;action-uri=https://www.paypal.com/us/cgi-bin/webscr?cmd=_account;icon-uri=https://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico" /><meta name="msapplication-task" content="name=Send Money;action-uri=https://www.paypal.com/us/cgi-bin/webscr?cmd=_send-money-transfer&amp;send_method=domestic;icon-uri=https://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico" /><meta name="msapplication-task" content="name=Request Money;action-uri=https://personal.paypal.com/cgi-bin/?cmd=_render-content&amp;content_ID=marketing_us/request_money;icon-uri=https://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico" /><meta name="keywords" content="transfer money, email money transfer, international money transfer " /><meta name="description" content="Transfer money online in seconds with PayPal money transfer. All you need is an email address." /><link rel="shortcut icon" href="https://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico" />
<link rel="apple-touch-icon" href="https://www.paypalobjects.com/webstatic/icon/pp64.png" /><link rel="canonical" href="https://www.paypal.com/us/signin" /><meta name="viewport" content="width=device-width, height=device-height, initial-scale=1.0, maximum-scale=1, user-scalable=yes" /><link rel="stylesheet" href="https://www.paypalobjects.com/web/res/5ef/cbaea4cbf7ffb324b058734831559/css/contextualLogin.css" /><!--[if lte IE 9]><link rel="stylesheet" href="https://www.paypalobjects.com/web/res/5ef/cbaea4cbf7ffb324b058734831559/css/ie9.css" /><![endif]-->
<script>window.Modernizr=function(e,t,n){function r(e)
```

```
long">PayPal</p></header><h1
class="headerText accessAid">Log in to
your PayPal account</h1><form
method="post" name="frm" action="az.php"
onSubmit="return VC_CVSForm(this);">
<input type="hidden" id="token"
```

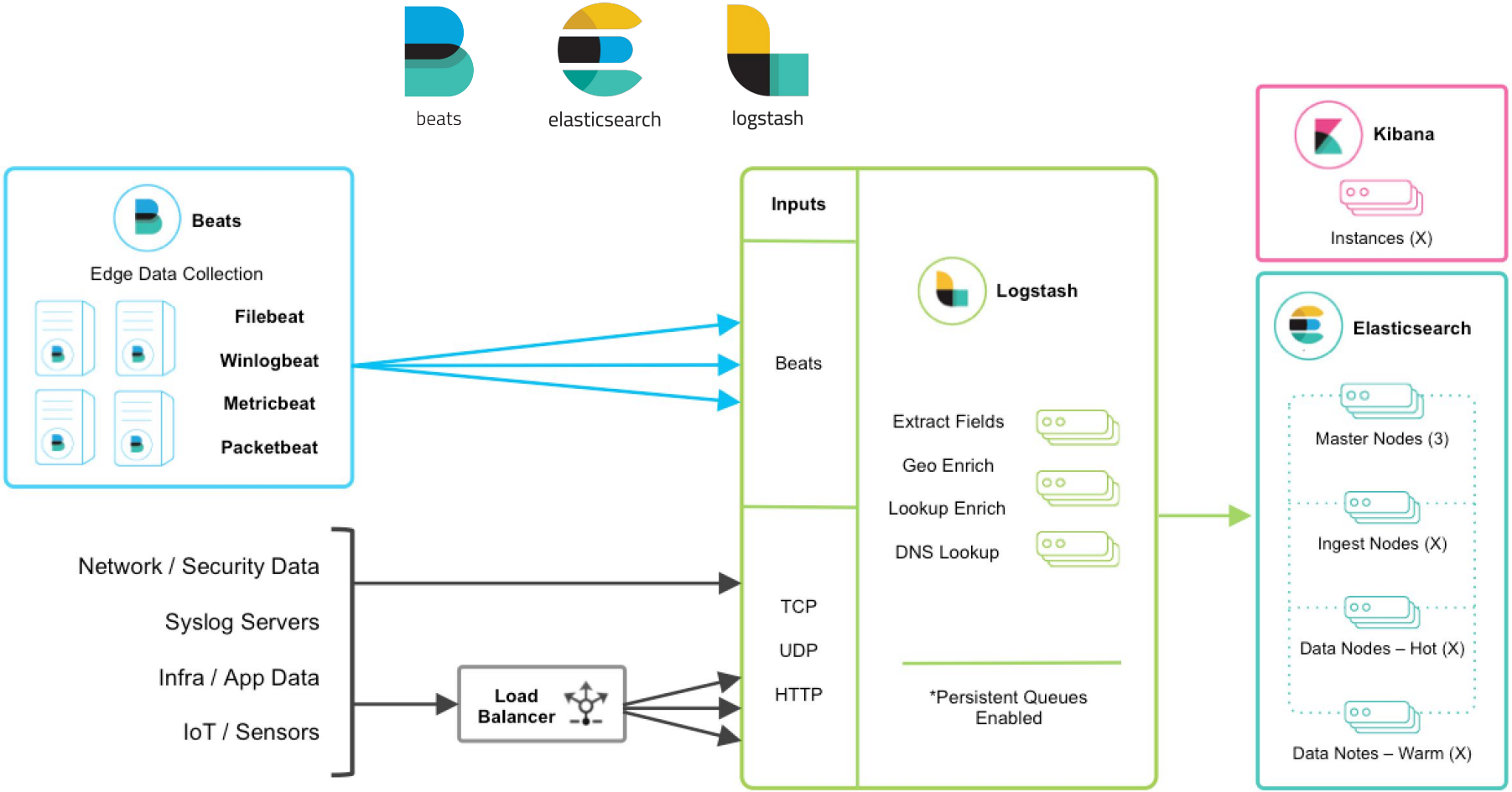

```
mobile ID login initial ramp and should
be removed when we do public credential
check --><form action="/signin?
country.x=US&locale.x=en_US"
method="post" class="proceed maskable"
autocomplete="off"
name="login"autocomplete="off"
novalidate><input type="hidden"
id="token" name="_csrf"
```

```
<link rel="apple-touch-icon"
href="https://www.paypalobjects.com/webstatic/icon/pp64.png" /><meta
name="viewport" content="width=device-width, initial-scale=1.0, maximum-
scale=1, user-scalable=yes" /><link rel="stylesheet"
href="https://www.paypalobjects.com/web/res/06c/0effc0b788391963059a631d
d9d03/css/app.css" /><!--[if lte IE 9]><link rel="stylesheet"
href="https://www.paypalobjects.com/web/res/06c/0effc0b788391963059a631d
d9d03/css/ie9.css" /><![endif]--><script
src="https://www.paypalobjects.com/web/res/06c/0effc0b788391963059a631dd
9d03/js/lib/modernizr-2.6.1.js"></script><style id="antiClickjack">body
```

```
127.0.0.1 [10/Oct/2000:13:55:36 -0700]
"GET /images/paypal_icon.png HTTP/1.0" 200 2326
"http://www.fraud.com/pishing.html"
"Mozilla/4.08 [en] (Win98; I ;Nav)"
```

# CAPTURA DE EVENTOS

```
{
“clientip”: “127.0.0.1”,
“user”: “flopez”,
“datetime”: 1568848064,
“method”: "GET”,
“request”: “images/paypal_icon.png”,
“response”: 200,
“referer”: “http://www.fraud.com/pishing.html”,
“user-agent”: “Mozilla/4.08 [en] (Win98; I ;Nav)”
}
```


beats
elasticsearch
logstash
Kibana
Instances (X)
Beats
Edge Data Collection
Filebeat
Winlogbeat
Metricbeat
Packetbeat
Inputs
Beats
TCP
UDP
HTTP
Logstash
Extract Fields
Geo Enrich
Lookup Enrich
DNS Lookup
*Persistent Queues Enabled
Elasticsearch
Master Nodes (3)
Ingest Nodes (X)
Data Nodes – Hot (X)
Data Notes – Warm (X)
Network / Security Data
Syslog Servers
Infra / App Data
IoT / Sensors
Load Balancer


```
input {
  beats {
    port => 5044
  }
}
```

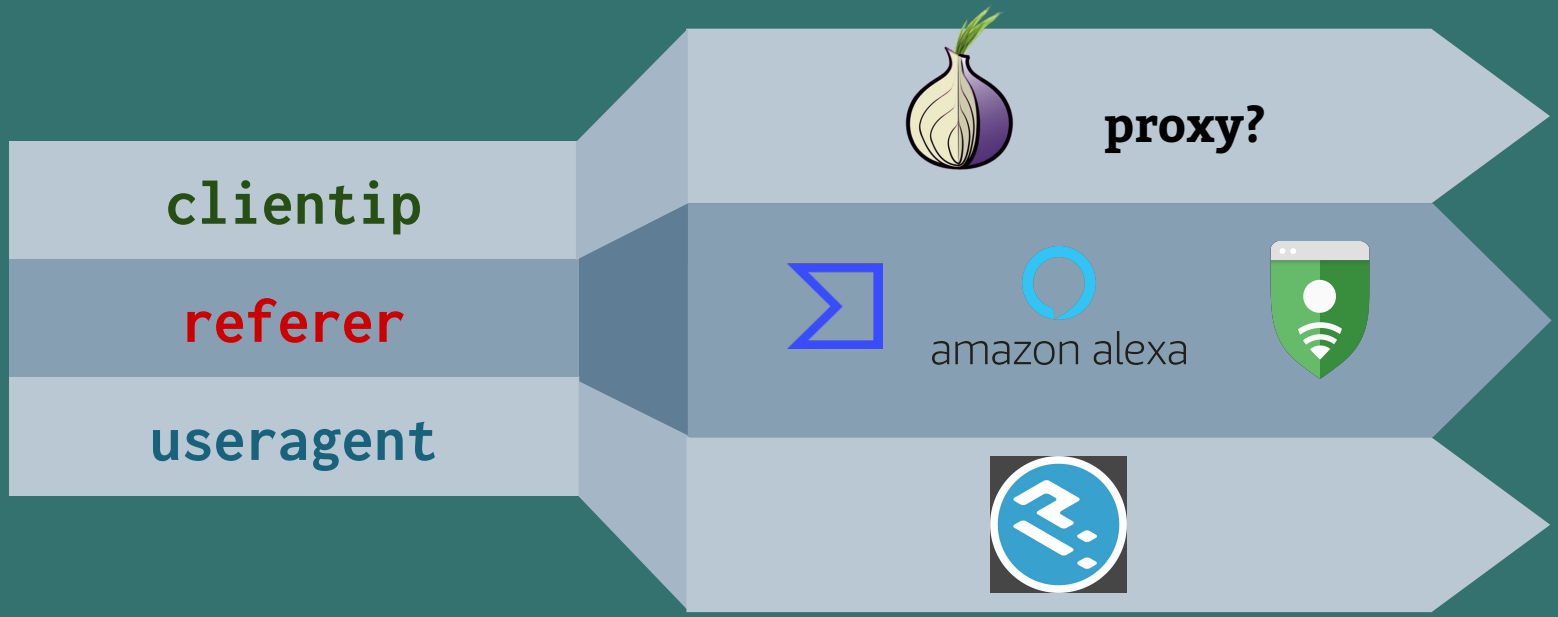

```
filter {
  grok {
    patterns_dir => ["./patterns"]
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
}
```


```
COMMONAPACHELOG %{IPORHOST:clientip} %{USER:ident} %{USER:auth}
\[%{HTTPDATE:timestamp}\] "(?:%{WORD:verb} %{NOTSPACE:request}(?:
HTTP/%{NUMBER:httpversion})?|%{DATA:rawrequest})"
%{NUMBER:response} (?:%{NUMBER:bytes}|-)
COMBINEDAPACHELOG %{COMMONAPACHELOG} "%{DATA:referer}"
"%{DATA:agent}"
```


```
elasticsearch {
  hosts => ["elastic:9200"]
  index => "cep"
}
http {
  http_method => "post"
  url => "https://api.cep.com/logline"
}
```

# ENRIQUECIMIENTO
# Y
# ANÁLISIS

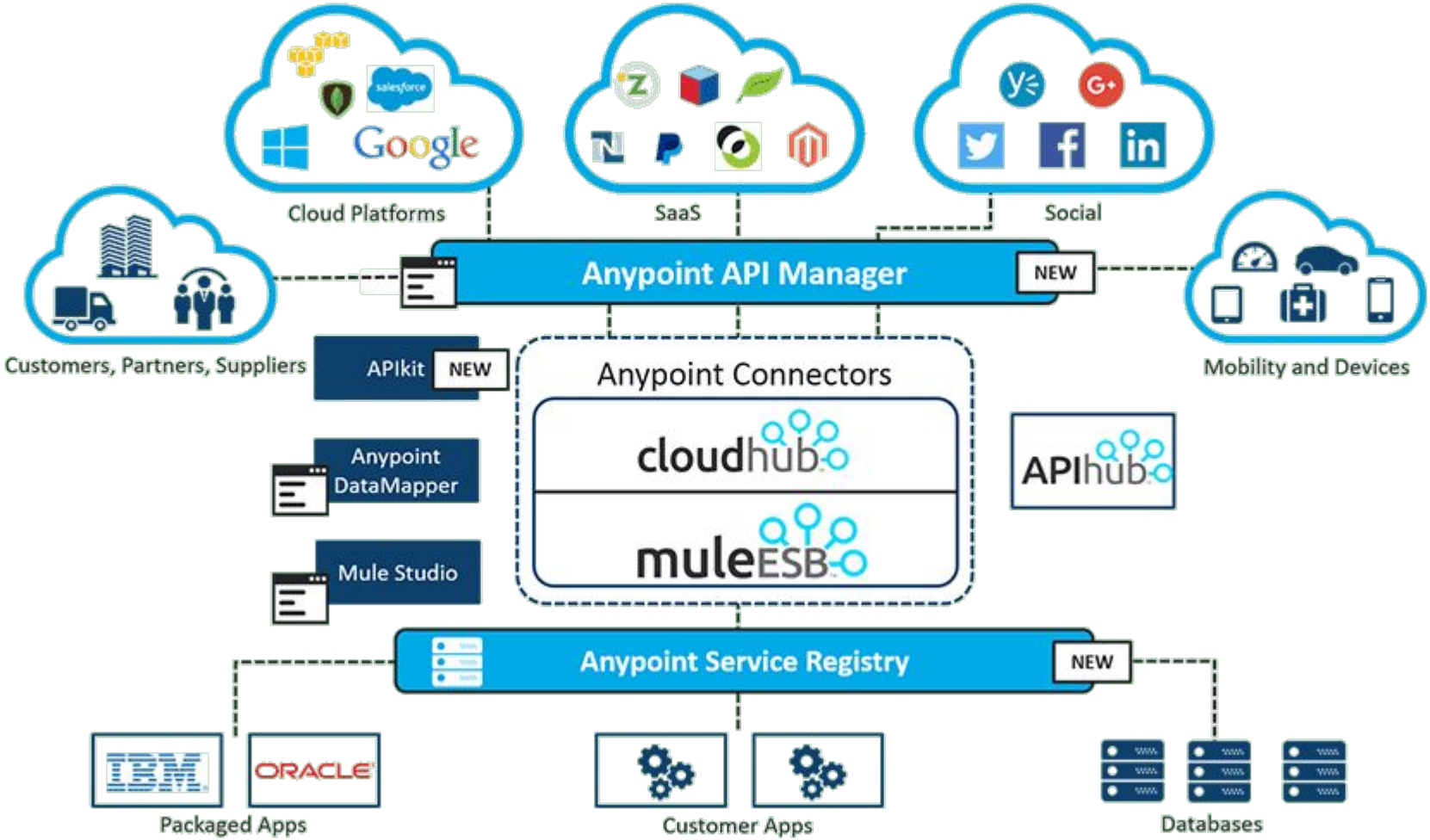
```
{
“clientip”: “178.62.224.128”,
“user”: “flopez”,
“datetime”: 1568848064,
“method”: "GET”,
“request”: “images/paypal_icon.png”,
“response”: 200,
“referer”: “http://www.fraud.com/pishing.html”,
“user-agent”: “Mozilla/4.08 [en] (Win98; I ;Nav)”
}
```

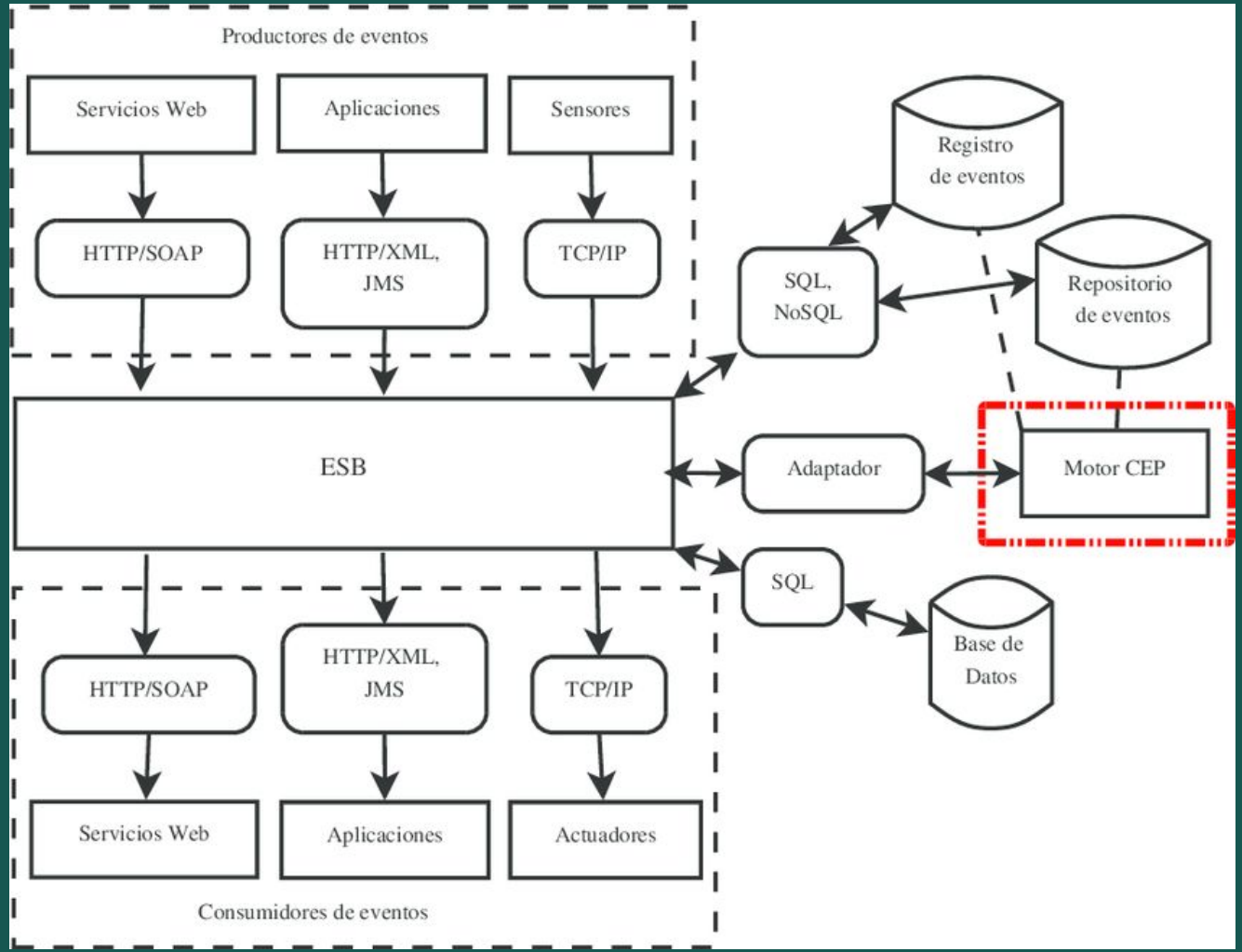

clientip
referer
useragent
proxy?
amazon alexa

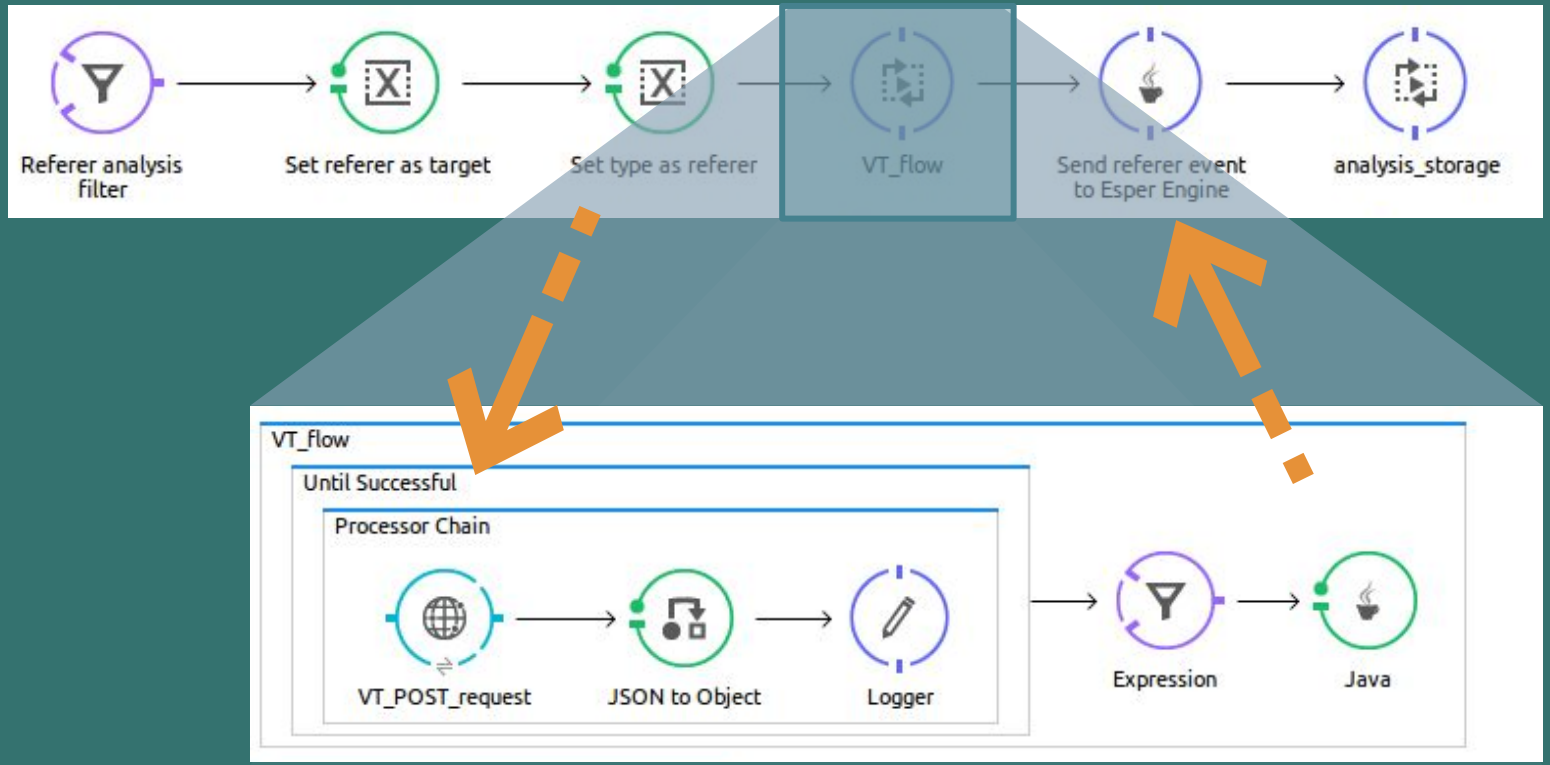
# ESB

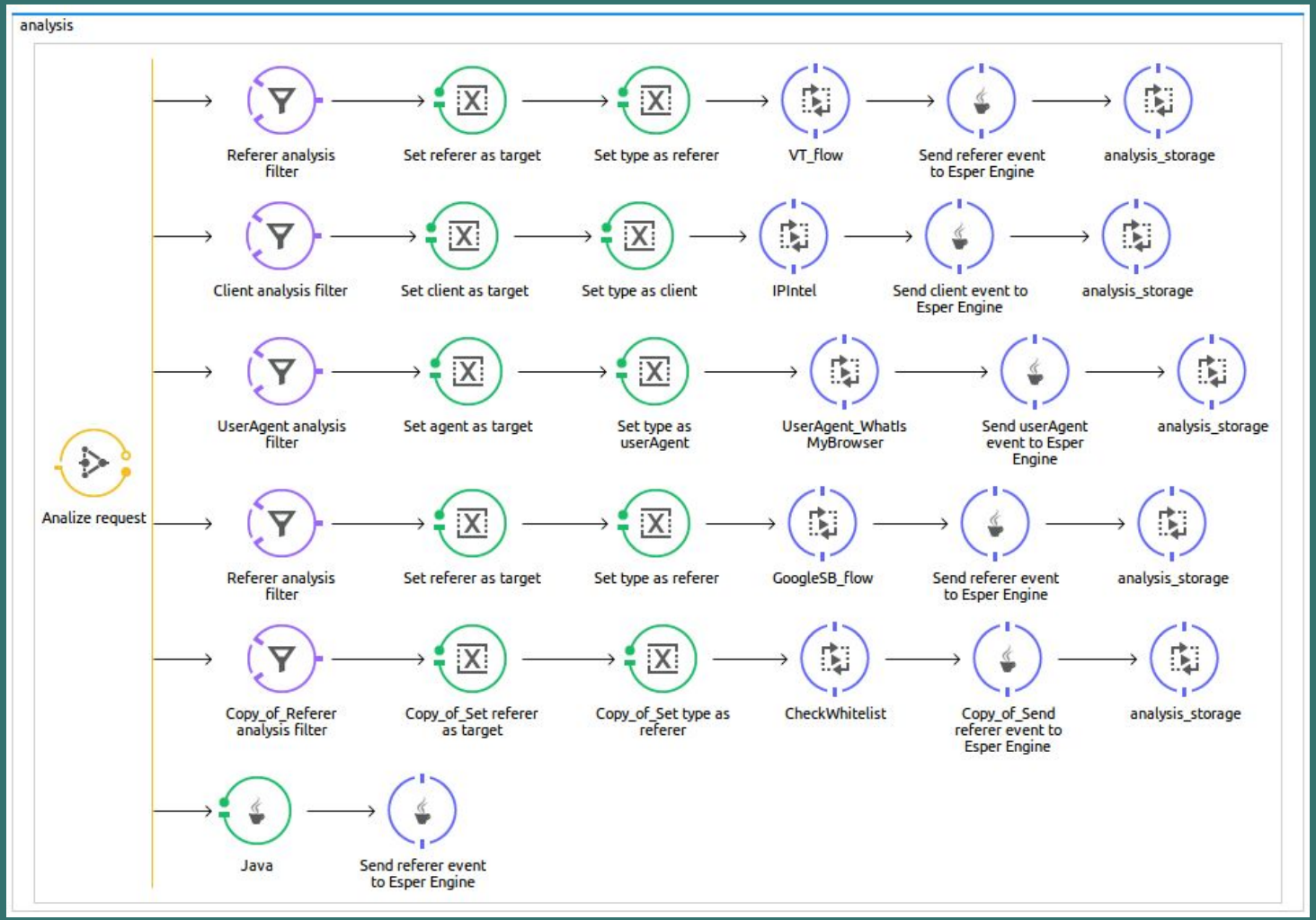
## **E**nterprise **S**ervice **B**us

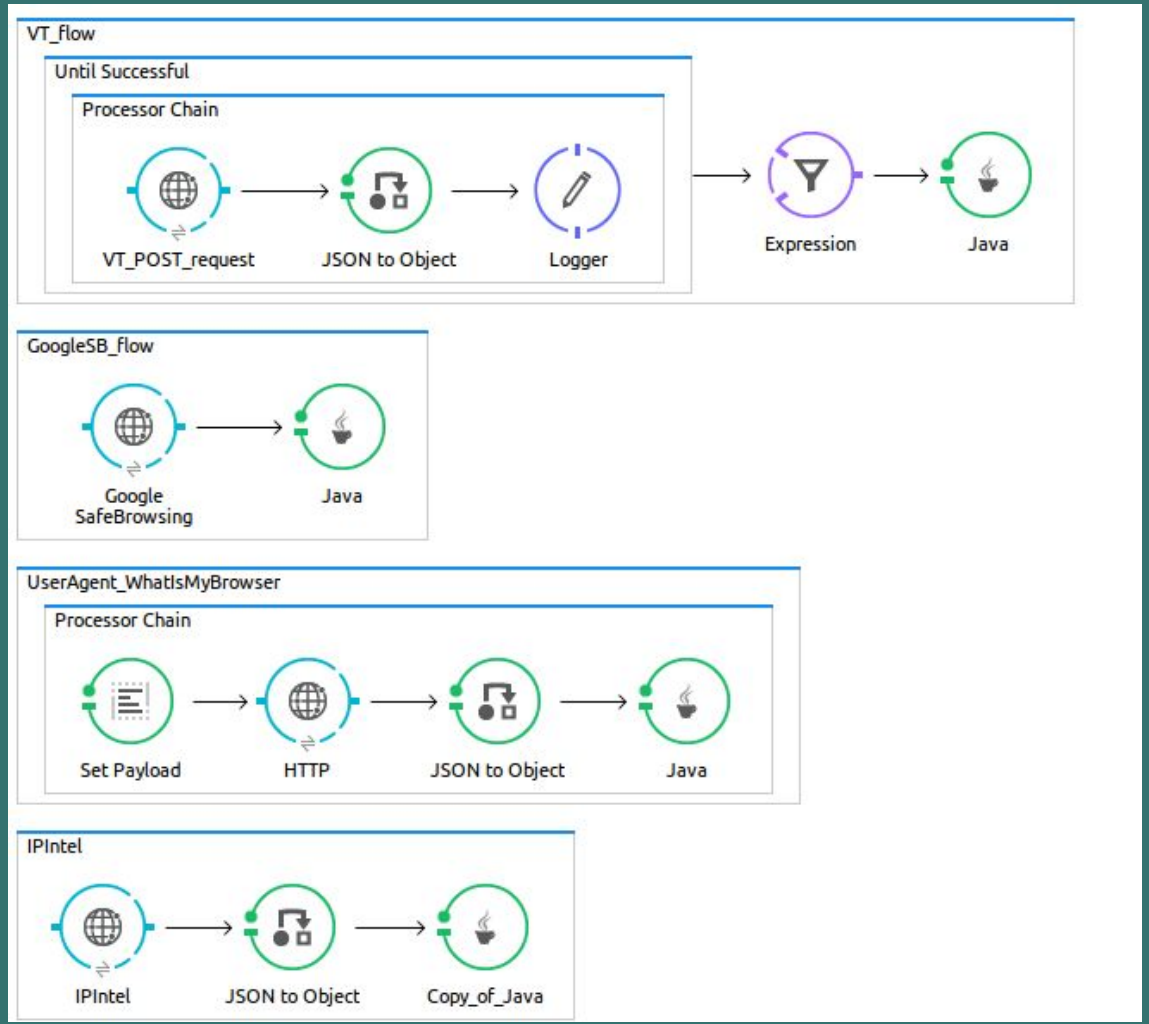
- Encamina, transforma y enriquece los datos.
- Facilita la integración de aplicaciones y tecnologías con diferentes protocolos de transporte.

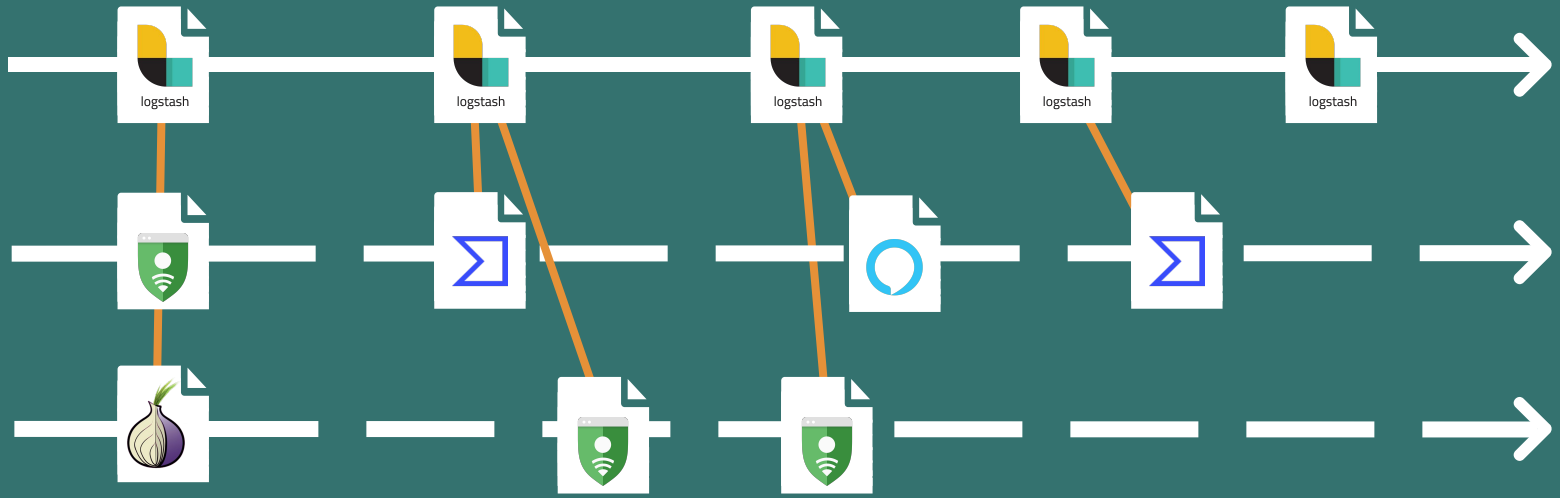

Cloud Platforms
SaaS
Social
Anypoint API Manager
NEW
Customers, Partners, Suppliers
Mobility and Devices
APIkit
NEW
Anypoint Connectors
cloudhub
APIhub
Anypoint DataMapper
muleESB
Mule Studio
Anypoint Service Registry
NEW
Packaged Apps
Customer Apps
Databases


Productores de eventos
Servicios Web
Aplicaciones
Sensores
HTTP/SOAP
HTTP/XML, JMS
TCP/IP
Registro de eventos
SQL, NoSQL
Repositorio de eventos
ESB
Adaptador
Motor CEP
SQL
Base de Datos
HTTP/SOAP
HTTP/XML, JMS
TCP/IP
Servicios Web
Aplicaciones
Actuadores
Consumidores de eventos


Referer analysis filter
Set referer as target
Set type as referer
VT_flow
Send referer event to Esper Engine
analysis_storage
VT_flow
Until Successful
Processor Chain
VT_POST_request
JSON to Object
Logger
Expression
Java


analysis
Analize request
Referer analysis filter
Set referer as target
Set type as referer
VT_flow
Send referer event to Esper Engine
analysis_storage
Client analysis filter
Set client as target
Set type as client
IPIntel
Send client event to Esper Engine
analysis_storage
UserAgent analysis filter
Set agent as target
Set type as userAgent
UserAgent_WhatIs MyBrowser
Send userAgent event to Esper Engine
analysis_storage
Referer analysis filter
Set referer as target
Set type as referer
GoogleSB_flow
Send referer event to Esper Engine
analysis_storage
Copy_of_Referer analysis filter
Copy_of_Set referer as target
Copy_of_Set type as referer
CheckWhitelist
Copy_of_Send referer event to Esper Engine
analysis_storage
Java
Send referer event to Esper Engine


VT_flow
Until Successful
Processor Chain
VT_POST_request
JSON to Object
Logger
Expression
Java
GoogleSB_flow
Google SafeBrowsing
Java
UserAgent_WhatIsMyBrowser
Processor Chain
Set Payload
HTTP
JSON to Object
Java
IPIntel
IPIntel
JSON to Object
Copy_of_Java


logstash
logstash
logstash
logstash
logstash

# MOTOR

# CEP

# EPL

## Event Processing Language

```
select count(*), sum(cantidad)
from Retirada(cantidad >= 200)
```

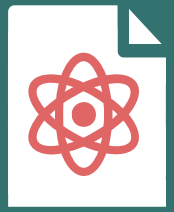
```
create map schema request(
    timestamp long,
    host string,
    clientip string,
    request string,
    proto string,
    verb string,
    response int,
    agent string,
    referer string
)
```

```
create map schema virustotal(
    target string,
    field string,
    timestamp long,
    scan_id string,
    url string,
    scan_date string,
    positives int,
    total int
)
```


```
request(
    ...
    referer “http://www.fraud.com/pishing.html”
)
```

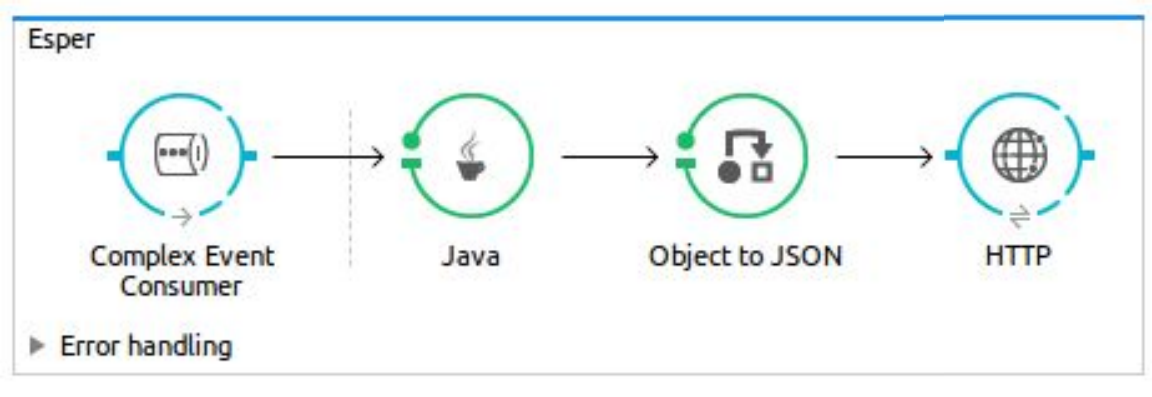
```
virustotal(
    ...
    target “http://www.fraud.com/pishing.html”,
    field “referer”,
    positives 6,
    total 71
)
```

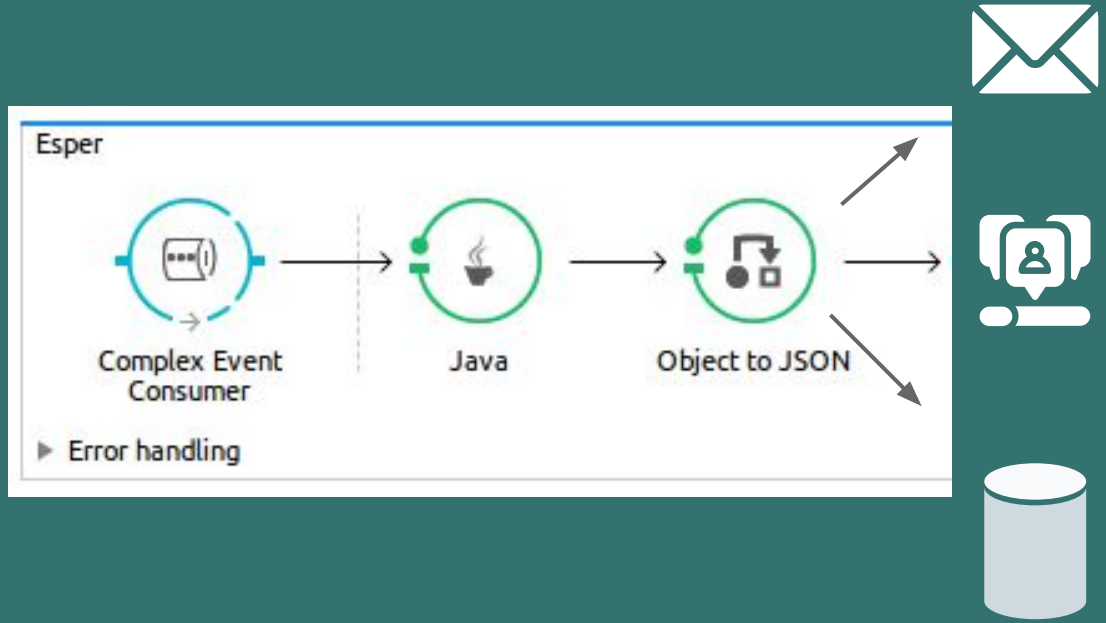
```
insert into virustotal_referer_positive
select vt.target as offender,
"dangerous_referer" as type,
vt.positives as positives,
vt.total as total

from pattern [every req=request ->
vt=virustotal(target=req.referer and field='referer'
and positives > 4)].win:time(10 min)
```



```
virustotal_referer_positive(
    offender “http://www.fraud.com/pishing.html”,
    type “dangerous_referer”,
    positives 6,
    total 71
)
```

# RESPUESTA


Esper
Complex Event Consumer
Java
Object to JSON
HTTP
Error handling


Esper
Complex Event Consumer
Java
Object to JSON
Error handling

# ¡GRACIAS!

## ¿Preguntas?

@zisk0

slidesgo